International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Integrating Visual Cryptography and Blockchain for Secure Online Voting System

Prajakta Bharsakle[1], Prof. Arundhati Chandorkar[2]

[1,2]Pune Institute Of Computer Technology, Pune, Maharashtra, India.

ABSTRACT

Securing the integrity, transparency, and privacy of voters in online elections is a significant concern in today's digital era. This study introduces an innovative solution by combining **Visual Cryptography** with **Blockchain technology** to develop a reliable and secure online voting system. Visual cryptography is used to convert each vote into multiple encrypted visual shares that can only reveal the original content when correctly combined, ensuring vote secrecy and protection against tampering. At the same time, blockchain offers a decentralized, transparent, and immutable ledger for recording votes, thereby removing reliance on centralized authorities and ensuring auditability. The proposed system guarantees end-to-end verifiability, secure voter authentication, and strong protection against vote manipulation or cyber threats. By merging these two technologies, the framework delivers a secure, transparent, and user-friendly voting experience that upholds the democratic process in a digital context.

Keywords: Secret Password, Secret Party Name, Verification, Vote Online, Cryptography, electronic voting; security; blockchain-based electronic voting etc.

INTRODUCTION

In a democratic nation like India, elections are fundamental to empowering citizens with the right to select their leaders through a transparent and fair process. Historically, India has relied on electronic voting machines (EVMs), which have streamlined the voting procedure compared to traditional paper ballots. However, these systems require voters to be physically present at polling stations, which limits accessibility in today's increasingly digital environment. To address this limitation, online voting platforms are being considered as a practical alternative, enabling voters to participate from any location during the specified voting period. While this innovation enhances convenience, it also raises significant concerns related to security, voter verification, and the integrity of the electoral process. It is essential to ensure that only authorized individuals can vote, while also protecting the confidentiality and accuracy of the cast ballots.

LITERATURE REVIEW

- **Visual Secret Sharing Using Cryptography**

Several studies have explored enhancing the security and efficiency of online voting systems. Naor and Shamir (1995) introduced Visual Cryptography (VC), a technique for sharing visual secrets using multiple image shares. Later, EEVCS (Embedded Extended Visual Cryptography Scheme) improved this by

embedding shares into meaningful cover images, increasing usability. However, traditional halftoning techniques used in EEVCS often produced poor visual quality.

- **Constructions and properties of k-out-of-n visual secret sharing schemes.**

The concept of k-out-of-n visual secret sharing schemes allows a secret image to be divided into *n* shares, where any *k* or more shares can reconstruct the image, but fewer than *k* reveal nothing. Initial constructions focused on the special cases of k = 2 and k = n, with further research extending to general values of *k*. These constructions are closely linked to MDS codes and maximum size arcs in coding theory.

- **Visual cryptography for general access structures**

A visual cryptography scheme enables a secret image to be split into shares, where only authorized groups (e.g., *k-out-of-n*) can visually reconstruct it by stacking the shares. This method requires no cryptographic computation. The paper proposes improved constructions with reduced pixel expansion and introduces graph-based access structures for flexible participant grouping.

- **Decentralizing Privacy: Using Blockchain to Protect Personal Data**

This paper proposes a decentralized personal data management system using blockchain to give users full ownership and control of their data, removing reliance on third parties. By treating blockchain transactions as access-control instructions rather than financial exchanges, the system ensures privacy, transparency, and trust. It highlights how blockchain can address broader trusted computing challenges beyond cryptocurrencies.

- **E-voting with blockchain: An e-voting protocol with decentralization and voter privacy.**

This paper proposes a blockchain-based e-voting protocol that ensures transparency, decentralization, and verifiability. It allows voters to update their votes within a set period and explores the practical benefits and challenges of using blockchain as a secure digital ballot box.

- **Blockchain-enabled e-voting**

Blockchain-enabled e-voting (BEV) allows secure and anonymous voting using encrypted keys and digital IDs. It helps reduce fraud, improve accessibility, and offers tamper-proof mechanisms, though it still faces technical and implementation challenges.

- **Secure Electronic Voting**

Electronic voting systems can boost voter turnout, especially among younger voters, and enhance the democratic process by supporting multilingual and flexible voting options.

- **Scantegrity: End-to-end voter-verifiable optical-scan voting**

Scantegrity II enhances traditional paper ballot systems by enabling voters to verify their votes using invisible, unique confirmation codes revealed during voting. These codes allow public verification without compromising vote secrecy.

- **VoteBox: A tamper-evident, verifiable electronic voting system**

VoteBox is uses distributed systems and cryptographic techniques to provide end-to-end verifiability, real-time monitoring, and voter challenge mechanisms, enhancing trustworthiness, transparency, and usability during elections

- **Blockchain and Visual Cryptography Based Secure Online Voting System**

This study explores the use of visual cryptography for developing a secure online voting system. It highlights the effectiveness of techniques like password-hashed schemes, threshold decryption, and VC for ensuring privacy, accuracy, and fraud prevention. The proposed system, implemented in Python, is efficient and runs on minimal hardware.

- **Securing E-Voting with Blockchain and Visual Cryptography**

Based on survey data and quantitative analysis, the findings confirm that blockchain offers a reliable and tamper-resistant alternative to traditional voting methods, addressing key issues like fraud and lack of trust.

- **A Hybrid Model for Blockchain-based Visual Secret Sharing in E-Voting**

This study proposes a blockchain-based EHR architecture that enhances the security and privacy of healthcare data, especially against quantum attacks. By combining ECDSA with Dilithium (a lattice-based signature scheme), it introduces a hybrid anti-quantum signature technique. The system ensures authorized access, and outperforms existing methods in terms of efficiency and security.

METHODOLOGY

1. Model Selection

- **Visual Cryptography Model**

Purpose: To ensure vote confidentiality without needing complex decryption.
Model: A vote (image or data) is split into two shares:
One share is given to the voter.
The other share is stored securely by the system.
Reconstruction: Overlaying both shares visually reveals the original vote without computational effort.

- **Blockchain Model**

Purpose: To ensure tamper-proof, auditable, and decentralized storage of voting records.
Model:
Each vote's metadata or hash (not the actual vote) is stored on the blockchain.
Smart contracts are used to validate vote submission, prevent double voting, and control access.
Platform: Ethereum (public), Hyperledger Fabric (private), or Polygon (scalable alternative).

- **Authentication Model**

Purpose: To ensure secure access and voter identity verification.
Model: Voters are authenticated using OTP, email
verification, or secure digital ID before casting votes.

2. Data Gathering

In the context of developing a secure online voting system that integrates Visual Cryptography and Blockchain, the data gathering process involves the creation and collection of synthetic, system-generated, and performance-based data. Since the system is being developed as a prototype and not deployed in a live environment, simulated data is used to replicate the functionalities of a real-world voting process. The main categories of data gathered are outlined as follows:

- **Simulated Voter Data**

To test the system functionality, a set of simulated voter profiles is generated. Each profile contains anonymized details such as voter ID, username or email, and the selected vote (e.g., Candidate A, Candidate B, etc.). This data is essential to simulate a real-time voting environment and validate the voting, authentication, and verification mechanisms of the system.

- **Visual Cryptography Share Data**

Visual Cryptography is used to convert each vote into two encrypted visual shares. During the data gathering phase, each vote is processed using a 2-out-of-2 secret sharing scheme, resulting in two image shares:

One share is stored with the voter,The other is stored by the system or election authority.
These shares are stored in image format (e.g., PNG) and used later for the vote reconstruction process by overlaying them.

- **Blockchain Transaction Records**

A blockchain ledger (e.g., Ethereum testnet or local Ganache network) is used to store metadata related to each vote. Rather than storing actual votes, the system stores:
Hash values of the visual shares,Voter ID (encrypted or anonymized),Timestamps, and Smart contract status logs.
This ensures the transparency, immutability, and traceability of the voting process. Blockchain logs serve as a verifiable proof of vote integrity.

- **System Performance Metrics**

During system testing, performance metrics are recorded to evaluate efficiency and responsiveness. Key metrics include:
Time taken for voter authentication,Time required for vote casting and share generation, Blockchain transaction processing time.
These metrics are captured using built-in system logging tools and are crucial for system evaluation and optimization.

- **Optional User Feedback Data**

In scenarios where usability testing is conducted with real users (e.g., for a demo or academic study), user feedback is collected using questionnaires. The aim is to evaluate user experience in terms of:
Ease of use,Perceived security,Confidence in vote privacy and system transparency.
This feedback supports the iterative refinement of the user interface and interaction design.

MODELING AND ANALYSIS

System Modeling

The proposed system is modeled by integrating Visual Cryptography for secure vote encryption and Blockchain Technology for transparent and tamper-proof storage. The system can be divided into four core modules:

1. **Voter Registration & Authentication Module**

Voter details are verified using unique identifiers (e.g., email or voter ID). A secure login mechanism ensures only eligible users can access the voting portal.

2. **Vote Encryption Using Visual Cryptography**

Each vote is converted into a secret image.A (2,2) visual cryptography scheme is applied to divide the vote into two shares:
One is given to the voter,The second is stored securely in the system.
Only when both shares are overlaid can the original vote be reconstructed.

3. **Blockchain-Based Vote Recording**

Metadata of each encrypted vote (hashes, timestamps, anonymized ID) is stored on the blockchain.
A smart contract is used to handle vote validation, prevent double voting, and confirm successful submissions.

4. **Vote Verification and Counting**

During tallying, the visual shares are overlaid to reconstruct the original vote image.
Voters can verify their votes via a blockchain ledger without revealing their identity.

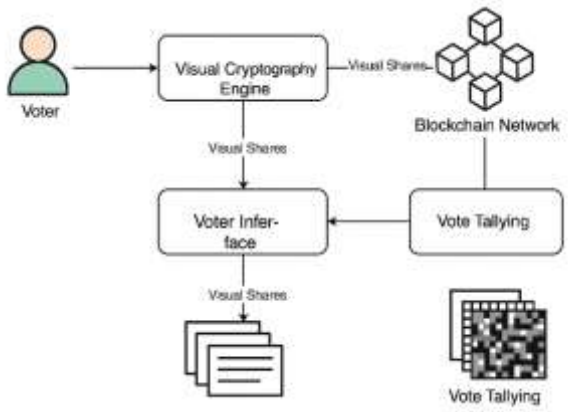

Fig 1: Architecture Diagram

Analysis

Aspect	Details
Security	Combines cryptographic image sharing with immutable blockchain records.
Transparency	Blockchain provides verifiability without compromising voter privacy.
Tamper Resistance	Visual cryptography resists vote manipulation, and blockchain ensures auditability.
Usability	Web-based interface with visual feedback; no need for cryptographic knowledge by users.
Performance	Minimal computational overhead using lightweight cryptographic methods.

- **Advantages of the Model**

Eliminates centralized vote tampering risk. Supports verifiable, anonymous voting. Ensures data confidentiality even if a share is leaked.

RESULTS AND DISCUSSION

The integration of Visual Cryptography and Blockchain significantly enhances the security, privacy, and transparency of online voting systems.

- **Security**: Visual Cryptography splits each vote into encrypted image shares, making it unreadable unless combined. Blockchain stores votes in a tamper-proof, decentralized ledger, ensuring data integrity.
- **Privacy**: Voter identity remains confidential through cryptographic techniques. Only authorized parties can reconstruct the original vote.
- **Transparency**: Blockchain allows all stakeholders to verify the votes without revealing voter identities, ensuring trust and auditability.
- **Decentralization**: No single authority controls the system, reducing risks of manipulation or central failures.
- **Performance**: The system handles large-scale voting efficiently, with minimal delays in vote recording and verification.

CONCLUSION

The integration of Visual Cryptography and Blockchain creates a highly secure, transparent, and tamper-proof online voting system. While there are challenges to overcome, particularly in terms of performance and complexity, the benefits in terms of security and privacy make it a promising solution for future electoral systems.

REFERENCES

1. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
2. https://www.cs.ru.nl/E.Verheul/papers/CDC1997/cdc1997. Verheul, E.R., & Van Tilborg, H.C.A. (1997). *Constructions and properties of k-out-of-n visual secret sharing schemes*.
3. https://citeseerx.ist.psu.edu/document. Ateniese, G., Blundo, C., De Santis, A., & Stinson, D.R. (2001). *Visual cryptography for general access structures*.
4. https://homepage.divms.uiowa.edu/~ghosh/blockchain.pdf Zyskind, G., Nathan, O., & Pentland, A. (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*
5. https://pure.royalholloway.ac.uk/ws/portalfiles/portal/30410016/e_voting_blockchain_2.pdf Hardwick, F.S., Akram, R.N., & Markantonakis, K. (2018). *E-voting with blockchain: An e-voting protocol with decentralization and voter privacy*
6. https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Blockchain_Enabled_2018.pdf Kshetri, N., & Voas, J. (2018). *Blockchain-enabled e-voting*.
7. https://www.infosec.aueb.gr/Publications/EUROSEC-2003.pdf Gritzalis, D. (2002). *Secure Electronic Voting*.
8. https://people.csail.mit.edu/rivest/pubs/CCCEx09.pdf Chaum, D., et al. (2008). Scantegrity: End-to-end voter-verifiable optical-scan voting.
9. https://www.usenix.org/legacy/event/sec08/tech/full_papers/sandler/sandler.pdf Sandler, D., Derr, K., & Wallach, D.S. (2008). *VoteBox: A tamper-evident, verifiable electronic voting system*.
10. https://www.usenix.org/legacy/event/sec08/tech/full_papers/sandler/sandler.pdf Rathi, M., & Sharma, A. (2021). *Blockchain and Visual Cryptography Based Secure Online Voting System*.
11. https://journalspub.com/wp-content/uploads/2025/04/23-37-Revolutionizing-E-Voting-with-Blockchain-A-Secure-and-Transparent-Framework-1.pdf
12. https://link.springer.com/article/10.1007/s40747-024-01477-1 Wang, Y., & Zhang, K. (2023). *A Hybrid Model for Blockchain-based Visual Secret Sharing in E-Voting*